AARP FRAUD WATCH NETWORK

GUIDE TO STOPPING ROBO-SCAMMERS

aarp.org/fraudwatchnetwork

Watchdog Alerts / Tips & Resources / Free for Everyone

AARP Fraud Watch Network

INTRODUCTION

The barrage of solicitations we get on our home landlines or, more recently, on our mobile phones are endlessly annoying. Sometimes the fake calls appear to be obvious with a number you don't recognize appearing on your caller ID. Increasingly though, illegal robo-callers use a technique called "spoofing" to make it look like the number is local, matching not only your area code but your three digit prefix. We've seen a dramatic increase in the number of illegal robo-calls using neighbor spoofing to get people to pick up the phone. And it works.

The number of robo-calls in the U.S. has gone up a whopping 219% since 2015, to 3.47 billion per month. Estimates suggest that by 2019, almost 50% of telephone calls to cell phones will be scams.
(Washington Post, September 2019.)

Not all robo-calls are from bad actors. Your pharmacy or your child's school use the technology to send automated messages to you. In fact, AARP uses the technology as a means to invite our members to join TeleTown Halls on issues of interest. Illegal robo-calls tend to be scammers or legal entities violating telecommunications laws.

Impostor calls, which often reach you with robo-call technology, are among the top complaints we hear at our AARP Fraud Watch Network Helpline and through our scam-tracking map. That is why it is so important to provide this guide on how to spot robo-scammers.

The best way to prevent fraud is through consumer education. Read this booklet and pass it onto a friend, so we can all know what to look for to avoid becoming victims of scammers.

TOP ROBO-SCAMS

The robo-scams described in this booklet have been reported to the AARP Fraud Watch Helpline or to federal regulators. Others we identified with the help of a service called Nomorobo, which blocks unwanted robo-calls. The robo-scams identified here are the most common scams going on at the time this booklet was written.

Each scam described in this booklet begins with The Pitch, which is a verbatim transcript of the exact words used by the robo-callers to get your attention and keep you on the line. The second part is The Catch, which is our best description of what will happen if you actually do stay on the line with the scammer. We know what happens, because fraud fighters have fielded these calls to find out what happens after the initial pitch. Finally, each description includes The Tip, which is our best advice for how to respond to these calls. Most of the time, the tip for how to respond is to simply not respond.

There is little doubt that as time moves on, the robo-callers and their techniques will change. This is why it is important to visit AARP's Fraud Watch Network to get updates on emerging scams. Visit aarp.org/fraudwatchnetwork to get the latest information about how to protect yourself.

A WARRANT FROM THE INTERNAL REVENUE SERVICE

THE PITCH:

"This is a final notice from the I.R.S. This message is to inform you that I.R.S. is filing a legal warrant under your name and your tax ID for the tax fraud and the investigating team of our department is investigating you and your family. We had tried to notify you regarding these issue in previous 6 months but we had never got response from you so it has been considered as an intentional fraud and lawsuit has been filed under your name by the United States government. You may call our department number 830-220-2074 extension 7. I repeat 830-220-2074 extension 7. Thank you."

THE CATCH:

At its peak, millions of Americans were receiving this type of call. Many people called the number back out of fear that they were in trouble with the federal government. When they called the number, they typically reached a "boiler room" somewhere in the world, where operators would try to convince them that they were from the IRS and to send them thousands of dollars they supposedly owed in back taxes. Often, these operators would get the victim to go to a large retail store and purchase gift cards. The victims would then read the card number to the scammer. That's the last the victim would hear from the "IRS."

THE TIP:

The IRS will never call you about past taxes without writing to you first. If you are concerned about such a call, contact the IRS independently and verify that you don't owe money.

THE TECH SUPPORT SCAM

THE PITCH:

"Someone is trying to hijack your computer and steal your personal information. If it's not fixed right away, then your computer will become obsolete and all of your credential information may get compromised. If you are the one who is using Microsoft Windows on your computer, then please call 201-299-4315 or press 1 now to speak with security team now. Please ignore if we called you by mistake."

"Still wondering why you receive a call from Windows security? Let me tell you, you received a call because we encountered suspicious activities going on with your computer. It seems to be someone is trying to hijack your computer and try to steal your personal credential information, and if it's not fixed right away, your computer will become obsolete. So please turn on the computer while we are connecting you to our expert."

THE CATCH:

When you press 1 to be connected to a "Microsoft expert" you are instead connected to a boiler room where a scammer posing as a Microsoft technician will tell you that there is someone trying to hack into your computer and they need to share screens with you to show you what exactly is wrong.

In order for them to share screens with you, they direct you to a website like "Helpme.net" or "fixit123.com". The scammer will give you a code to enter and when you do that, they will have access to your computer. Then they will tell you about all the things that are "wrong" with your machine and tell you they can fix it by charging you a fee of between $299 and $999 depending on how much they think they can get out of you.

THE TIP:

Never allow someone who calls you on the phone to take over your computer. If you are concerned that there is something wrong with your computer, take it to a Microsoft or Apple retail store or somewhere that has a certified technician.

"RELIEF" FROM THE PAIN MANAGEMENT CENTER

THE PITCH:

"I am from Pain Management Center. I'm a medical verification specialist. We work directly with your health insurance company, and we have on file that you are qualified to receive these benefits. And since this is from your health insurance, this is no cost. And my job here is to make sure that these updated benefits are offered to you, and to make sure this will be safe and beneficial."

"One benefit is what we call PlasmaFlow. This is just updated from your health insurance this month. It's a device that you simply need to attach on the area where the pain is located. The pressure created by the pump pushes fluid in your extremities, which allows blood to flow freely, and this PlasmaFlow will not only improve blood flow, they also reduce swelling and pain. The good thing it's completely portable, no wires or bulky devices; you can place it anywhere the treatment is needed. And along with that is what we call the "new technology brace." This new technology brace is not this same brace before. It's made of breathable mesh material. It's thin and lightweight, no bulky metals or plastic on it. So this brace aims to decrease the intensity of pain symptoms by relieving pressure on the site, and providing you with stability and support."

THE CATCH:

This scam targets Medicare enrollees and is designed to capture as much personal information about the victims as possible under the guise that they will receive a free neck brace or pain-relieving pump of some kind. They will require that you provide your Medicare number and may even send you a cheap version of a neck or knee brace, but then bill Medicare for thousands of dollars more than it is worth. Even worse, you have now given questionable characters your personal information that they may also use to steal your identity and open new credit card accounts in your name.

THE TIP:

Avoid engaging with calls from strangers who ask you personal questions about your health. If you have knee or neck pain, consult with your doctor about possible solutions.

THE AMAZON BUSINESS OPPORTUNITY SCAM

THE PITCH:

"Hi, this is Sally Martin calling back. This is regarding your request to make money from home. We've been trying to reach you because you can make up to $750 dollars a day as an authorized Amazon affiliate guaranteed. There's no experience or computer knowledge required. We provide the training. Again, you can make up to $750 dollars a day guaranteed as an authorized Amazon affiliate. Amazon has made this unique opportunity available. No computer experience or knowledge required and we provide the training. Call now at 1 800-490-5185. Positions are filling quickly you do want to call within the next 48 hours again that number is 1-800-490-5185. Thank you."

THE CATCH:

Amazon doesn't robo-call people to offer them job opportunities. More likely, it is a scammer, or at the very least a shady operator who purchased a lead list of people who have shown an interest in work-at-home opportunities. When you call the number they provide, you are likely to get a pitch to pay thousands of dollars for help designing a website where they will claim you can make thousands selling products from the comfort of your own home.

THE TIP:

While many people have success at starting and running their own online businesses, law enforcement has brought numerous actions in recent years against scammers who are selling this idea to unknowing consumers. Taking a solicitation by phone as your impetus to start your own online business is risky at best.

SOCIAL SECURITY TROUBLE

THE PITCH:

"Hello, this is Officer Kevin from the Social Security fraud department. Your Social Security number has been compromised and there is an enforcement action which has been started against your Social Security number. We request you contact your case officer at 415-796-0832. I repeat 415-796-0832. Thank you. Have a good day."

THE CATCH:

The scammer will also pose as an official from the Social Security Administration to scare people into handing over their personal identifying information like Social Security number, date of birth and other personal details. The scammer may call several times if they don't receive an immediate answer. The frightened target calls the number and gives their personal information to the scammer, who then uses it to try to open credit cards in the victim's name, or take other actions in an attempt to steal their money or their identity.

THE TIP:

If you receive a call like this, contact the Social Security Administration before calling the person who contacted you and verify if there is a problem with your account. Call 1-800-772-1213 or set up online access to your information at www.ssa.gov/myaccount.

THE JURY DUTY SCAM

THE PITCH:

"This is Ms. Rogers from the Courthouse calling. Our records indicate you were summoned to court three weeks ago to serve on jury duty and you failed to show up. Unless you agree to pay the mandatory fine of $989, we will have no choice but to execute a warrant for your arrest."

THE CATCH:

The courts simply do not call and threaten arrest for missing jury duty. In the vast majority of cases, courts send jury notices by mail, and use the same process to contact individuals who may have not responded to the notice.

THE TIP:

The best thing to do if you receive a call like this is to simply hang up and report it to the local sheriff or police. If you are concerned that you might actually owe money, independently contact the law enforcement agency or court that supposedly called you and verify that you do not owe money and haven't missed a court date or jury appearance.

THE FACEBOOK COMPROMISE

THE PITCH:

"This call is from Facebook. We are sorry to inform you that your account was recently compromised. To avoid your account suspension, press 1 to review verifier account or dial 184-487-3605 extension 7. Otherwise your account will be suspended within 24 hours."

THE CATCH:

This is a variation of the tech support scam. If you follow the prompts and press 1, the "representative" will likely ask you for your login credentials or other personal information. They may tell you that you have a virus on your computer that they can remove by taking over your computer remotely and charging you a fee. If you do this, they can install a virus or malware that will allow them to take over your social and financial accounts or even monitor your activities.

THE TIP:

If you have concerns about your account, log on and click on "Settings" to review your privacy settings. If you think someone has compromised your account, establish a new password. Avoid going online to search for "Facebook customer service" and then call one of the numbers listed. A bevy of scammers are online just waiting for us to do that.

THE GOVERNMENT GRANTS SCAM

THE PITCH:

"From United States Government Grants Department this is an important message for you. We congratulate you that you have been qualified to receive a royalty money of $14,750.00. To know the reason why you are qualified your call will be forwarded to senior accounts manager and to claim this money press 1 or call back 170-784-0538 extension 5 I. Repeat 170-784-0538. This call is from United States government Grants Department. This is an important message for you. We congratulate you that you have been qualified to receive a royalty money of 14750 dollars to know the reason why you are qualified your call will be forwarded to senior accounts manager and to claim this money press 1 or call back 170-784-0538.

THE CATCH:

There is no United States Government Grant office that will just call you up and tell you you're eligible to receive money from the federal government. The government does provide grants, but rarely to individuals. The catch is they will tell you to pay a tax or an administrative fee before you can receive your award. Once you pay the fee, you will never hear from the caller again.

THE TIP:

The best thing to do is delete this message or hang up on the caller.

THE VETERANS CHARITY SCAM

THE PITCH:

"If you have been thinking about donating your car, real estate, or timeshare to charity, please consider donating to Veterans of America. Donations are tax deductible and all real estate donations are deductible for full market value. We accept all types of vehicles, boats, real estate, and timeshares. If you would like to talk to someone about donating now press 1. To be taken off of our list and not contacted again press 9. Thank you."

THE CATCH:

A variety of robo-scams target donations to veterans' organizations. While many are legitimate, others are in the business of soliciting donations and then keeping 90% of the money for the cost of fundraising. That means if you give $100, the veterans organization gets $10 and the fundraiser doing the calling keeps $90. That is, if the organization is a real charity. Some are completely fictitious.

THE TIP:

Ask the caller how much of your donation will go directly to the charitable purpose and how much will go to the professional fundraiser. You can contact your state Attorney General or Secretary of State and verify the information before giving. You can also research a charity at www.charitynavigator.org before donating to it, so that your contribution actually goes to real charities that need your support. Also, consider establishing a set list of charities that you will give to each year. For any charity that isn't on your list, you can simply explain that you have made your charitable giving plans for the year. Also, avoid pressing 9 to be taken off the list – that simply tells the scammer your number is live and they will try again.

GREETINGS FROM THE CREDIT CARD AWARD CENTER

THE PITCH:

"This is not a solicitation call. This is the credit card holder award center from Visa Master Card. We have been monitoring your credit card account for the last 6 months. Congratulations on your excellent payment history you now qualify for a 0 percent interest rate on all your credit card accounts. This is a limited time offer and you must respond by pressing 1 now to speak to our qualification department and complete the process. The qualification process can be completed in a few minutes. 2468."

THE CATCH:

No matter how strongly the robo-caller declares this is not a solicitation call, it is a solicitation call. The caller will likely ask you to provide personal information, which may or may not be used to get you a lower interest credit card.

THE TIP:

If you are interested in getting a lower interest rate on your credit cards, the best thing to do is to shop around for competitive rates. As for the calls offering this "deal"? Simply hang up.

THE BREAST CANCER CHARITY SCAM

THE PITCH:

"Is the lady of the house there? Is the lady of the house there? Is the lady of the house there Lou finally a real person. This is Sam calling on behalf of the breast cancer charities of America. Didn't mean to bug you; we just wanted to let you know we're mailing out the envelope for this campaign you know for that "I go pink" drive to help the ladies directly with their fight against breast cancer. Of course the amount's up to you. Just want to make sure if you get it in the mail you can send something back to help the ladies. Is that OK?"

THE CATCH:

Just like appeals to support veterans, there are many legitimate charities raising money for woman's breast health and preventing breast cancer. However, many questionable fundraisers use this worthy cause to bring in millions of dollars that go to the fundraisers.

THE TIP:

Ask the caller how much of your donation will go directly to the charitable purpose and how much will go to the professional fundraiser. You can contact your state Attorney General or Secretary of State and verify the information before giving. You can also research a charity at www.charitynavigator.org before donating to it, so that your contribution actually goes to real charities that need your support. Also, consider establishing a set list of charities that you will give to each year. For any charity that isn't on your list, you can simply explain that you have made your charitable giving plans for the year.

CONCLUSION

Despite the many benefits of new and transformational technologies, a down side is that it has enabled thousands of scammers cheaply and easily to bombard our phones with an avalanche of robo-scams. This booklet has outlined some of the most common robo-scams blasting into our homes right now. From IRS impersonators to fake Microsoft and Apple technicians to scammers posing as the local court system, there is no shortage of impostors out there. And if past is prologue, the scams will continue to change as law enforcement and consumers catch on to the tactics being used in efforts to defraud us.

To explore more information about how to stop robo-scams, visit the AARP Fraud Watch Network at www.aarp.org/fraudwatchnetwork where you will find useful information on how to protect yourself and your family from scammers' tactics.

If a scammer has approached you or someone you love, call the AARP Fraud Watch Network Helpline at 877-908-3360 to speak with volunteers trained in fraud counseling.

To report fraud, visit ftc.gov/complaint. While reporting won't help you with restitution, it will help law enforcement identify trends that can result in taking down the bad guys.

aarp.org/fraudwatchnetwork

Watchdog Alerts / Tips & Resources / Free for Everyone

AARP®

Fraud Watch Network

D20469 (1218)